Editors: Pavel Gladyshev, pavel.gladyshev@ucd.ie | Joshua James, joshua.i.james@pm.me

Dealing With COVID-19 Network Traffic Spikes

Mahmoud Said Elsayed, Nhien-An Le-Khac, and Anca Delia Jurcut | University College Dublin

The novel severe acute respiratory syndrome coronavirus 2 and its associated disease, COVID-19, have increased the amount of time that people spend working from home and in social isolation. In 2020, the number of users worldwide who relied on the Internet for work, education, and entertainment increased significantly. This growth is causing a substantial rise in bandwidth usage, with a sudden spike in the number of cyberattacks, such as distributed denial of service (DDoS). The situation is accelerating IT infrastructure providers' migration toward new technological innovations, such as software-defined networking (SDN). Compared to traditional architectures, can SDN-based networks flexibly solve security and management problems to cope with the new challenges?

Digital Object Identifier 10.1109/MSEC.2020.3037448
Date of current version: 25 January 2021

Critical Services

Due to the COVID-19 pandemic, governments worldwide have been providing self-quarantine and social distancing guidance to limit the spread of infection, leading many organizations and employees to shift to remote working solutions. In response, the use of online video meeting applications, such as Zoom, Google Meet, and Skype, increased considerably.[1] According to a 2020 Nokia report,[2] video conferencing traffic is up 700% in the United States compared to February 2020. Similarly, broadband provider BusinessWire has counted a 30% rise in data traffic and a 50% jump in voice traffic on its network since mid-March.[3] There has been a reported 45% increase in communication traffic from applications such as WhatsApp, Teams, and Skype.[4] Simultaneously, voice calls have doubled in number, and overall voice usage is 45% higher. The increase in used bandwidth forced Internet companies, such as Amazon, YouTube, and Netflix, to reduce the quality of their streaming services. The goal was to ease the pressure on telecommunication networks. As a result, several organizations established pandemic-specific policies and procedures to maintain their essential services and products.

DDoS attacks have also increased significantly during the pandemic. According to a Bitglass remote work report,[5] 84% of organizations support remote work capabilities. Consequently, 65% of organizations allow managed applications to be accessed by personal devices. However, many organizations find it difficult to secure remote networks, and 41% of companies have not taken any steps to expand secure access for their remote workforce, according to Bitglass.[5] This article investigates

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/21©2021IEEE

how SDN can handle the complexity and overhead in legacy network architectures.

What Is SDN?

SDN simplifies system management and configuration to introduce new abstractions in networking. SDN facilitates the execution of policies and the dynamic control of networks through a centralized controller. The key concept behind the SDN paradigm is the separation of control and data functions from network devices, such as routers and switches.

The key concept behind the SDN paradigm is the separation of control and data functions from network devices.

The SDN architecture consists of three planes: data, control, and application, as depicted in Figure 1. The data plane contains the network equipment and is responsible for the flow from the source to the destination networks. The network plane does not rely only on physical devices, such as routers and switches; it can contain software-based devices, including virtual switches.

The control plane acts as the brain of the SDN architecture and contains one or more controllers. The primary function of the control plane is to execute network policies. The application plane encompasses various functions, such as load balancers, detection systems, and network monitors. Applications interact with the SDN controller to utilize an abstract view of the network for internal decision-making processes.

Why SDN?

Compared to traditional systems, SDN-based networks can flexibly solve security and management problems. SDN provides the concept of programmability to enable new network functions. Many network and security tasks, such as intrusion detection, network monitoring, and load balancing, can be used according to requirements. Moreover, modifying software applications is much easier than manually reconfiguring each network device. These benefits enable enterprises to meet ever-changing business demands without purchasing extra expensive network devices. Therefore, SDN can simplify the overall network design and enhance interoperability. In addition, network operators always use a management console or a command-line interface to configure devices in the traditional network. These interfaces lead to a configuration bottleneck and much manual effort. In contrast, SDN's virtualized behavior can simplify operators' overall network management through the centralized controller.

The collection of powerful and diverse SDN functions encouraged real-world network environments, such as Google and Facebook, to apply the technology in their data centers. Moreover, SDN can enable robust services in wireless network environments.[6] Breaking network infrastructure into tractable pieces helps SDN surmount the limitations of the current system architecture, facilitating evolution and simplifying management.

SDN Security Enhancements

The centralized location of the SDN controller can provide more flexible deployments of network monitoring and ease the implementation of intrusion detection systems against attacks.[7] The SDN controller can send request messages to collect statistics information from any network device (i.e., the data plane). We can understand the routing information and overall network topology by analyzing flow requests from the collected devices. Moreover, the SDN network's holistic view can help us develop security applications without exerting much effort.[8]

To deploy intrusion detection systems against DDoS attacks

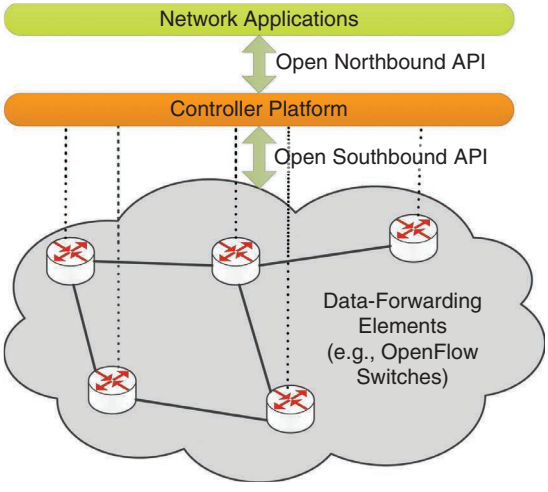

Figure 1. The SDN architecture. API: application programming interface.

in traditional architectures, we need to monitor as many network links as possible. This is because the source of attacks is unknown (e.g., botnets). However, the centralized controller's global view in SDN facilitates DDoS detection by instructing network devices to pass the flow traffic to the controller for further inspection without installing additional equipment. In terms of any suspicious traffic patterns, the controller generates alerts and instructs the SDN switches to block the source.

SDN Traffic Management

There has been a dramatic increase in the network load since people began working remotely, and countless students rely on remote learning. Hence, automated policy-based traffic management is more critical than ever to address the surge of bandwidth demand. In general, there are different types of applications that consume high amounts of bandwidth. Thus, fair access to critical services is an absolute requirement.

For example, real-time applications, such as voice over Internet Protocol, are more sensitive to delay. In contrast, other applications, including video conferencing, need a specific bandwidth for their traffic, thereby requiring special handling, i.e., higher priority. The quality of service (QoS) has been commonly applied in the traditional network, which faces many difficulties in guaranteeing the QoS for different applications. For example, applying a strict QoS can consume bandwidth overprovisioning.

Automated policy-based traffic management is more critical than ever to address the surge of bandwidth demand.

There are particular network protocols, such as integrated services and differentiated services, that are mainly used to establish the QoS in networks. However, these methods are not flexible enough. They require a complicated and expensive implementation to achieve better management, or they become coarse-grained in the case of simple deployments. Compared to traditional architectures, the SDN network's global view facilitates the configuration of the QoS since SDN simplifies system management through the efficient use of resources. SDN can control and modify the entire network's characteristics with dynamic, automated SDN programs written by operators to optimize assets.

Network operators can quickly implement automated QoS management frameworks using packet scheduling, queue management, and resource reservation. They can configure different routing algorithms with the help of OpenFlow instead of using the typical shortest path to improve QoS-motivated routing. SDNs can predict future behaviors, and they enable very low-level counters, such as per queue, per table, per port, per meter, and per packet, enabling operators to monitor network dynamics.[9]

DDoS Attack Case Study

The new architecture of SDN (i.e., decoupling the data plane from the control plane) creates DDoS attack surfaces that did not exist in conventional networks.[10] However, the SDN controller becomes a single point of failure and a prime target for attackers to exploit. An attacker can bring down an entire network or disrupt its regular operation by attacking the controller. Therefore, it is essential to understand and investigate these attacks' potential impact from the bad actors' perspective.

This section provides an experiment studying DDoS attacks' effects and their consequences on the SDN controller's load and throughput. The experiment was performed using the Mininet simulator tool and the OpenDaylight controller platform. They were installed on separate virtual machines. The simulation network topology is depicted in Figure 2. The system under test consists of a set of hosts attached to OpenFlow switches in a tree topology. The command that was used to create the network topology is:

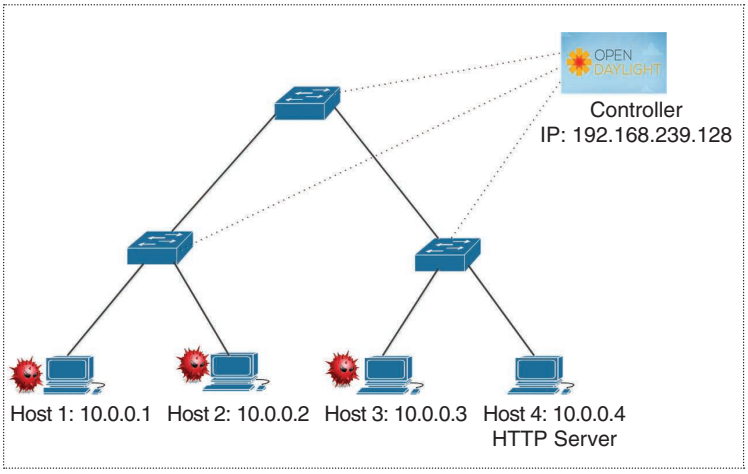

Figure 2. The network topology.

sudo mn –topo tree,2 –mac –controller=remote,ip=192.168.239.128,port=6633 –switch ovs,protocols=OpenFlow13.

Here, hosts h1, h2, and h3 are attackers, and their objective is to generate a maximum workload for the controller. A maximum load is produced by creating an enormous number of requests. As a result, many OpenFlow packet-in messages are being sent to the controller and eventually consume its computing resources. H4 acts as a simple HTTP server that will listen on port 80. The simple HTTP server can be established by running the following command on the h4 terminal:

python -m SimpleHTTPServer 80.

Hping3 tool is used to flood the victim server and send the attack packets. The experiment test is measured for 60 s, and the DDoS flooding attacks last for 10 s.

Figure 3 shows the CPU load of the SDN controller. The network throughput upon executing the flooding attack is illustrated in Figure 4. It can be seen that there is a significant increase in the CPU load due to the flooding attacks, as a function of the attack packet rate. Before the attack, the controller load and the network throughput are low because there are only a few communications between the controller and the OpenFlow switches. During the attack, the controller is flooded with many requests, raising the throughput and eventually exhausting and plunging the controller. The overall conclusion is that an attacker controlling a few hosts can completely exhaust the network resources or degrade the system's performance if many attack flows are directed to the SDN controller. Therefore, enhancing the security of the controller is an essential issue in the SDN system.

The COVID-19 pandemic has had a massive impact on Internet usage. The global SDN market expects to achieve significant growth to keep pace with the rising traffic levels. SDN brings flexibility to network infrastructure, unlike traditional systems. It transforms today's network into flexible and programmable platforms by isolating logical intelligence from system devices. Such features enable a better response to network changes, whether they stem from increased legitimate user access or DDoS attacks. SDN also provides features that are useful for automated decision making during new and unexpected events. This flexibility facilitates real-time responses to changing network conditions. SDN, however, is not perfect.

SDN also provides features that are useful for automated decision making during new and unexpected events.

An SDN controller is a single point of failure from which an attacker can manipulate an entire network. In case an attacker gains access to the SDN controller, he or she can drop or redirect all incoming traffic. In the worst case, an attacker can start a new assault against other targets. Furthermore, the SDN controller is susceptible to DDoS attacks. All unmatched traffic by SDN switches is forwarded to the controller for further processing. An attacker can generate useless traffic to deplete the controller's resources or cause packets latency.

Data plane devices are also vulnerable to DDoS attacks. Since the data switches have a limited buffer size and a restricted flow table, an attacker can flood a network with large payload packets to fill

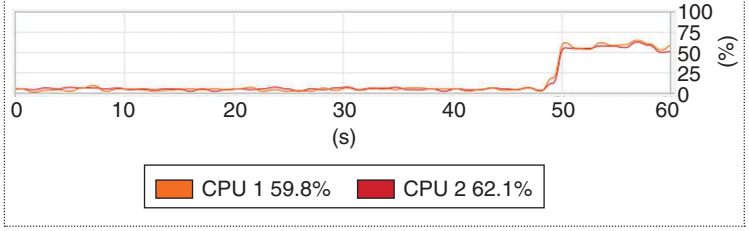

Figure 3. The CPU load before and after DDoS flooding attacks.

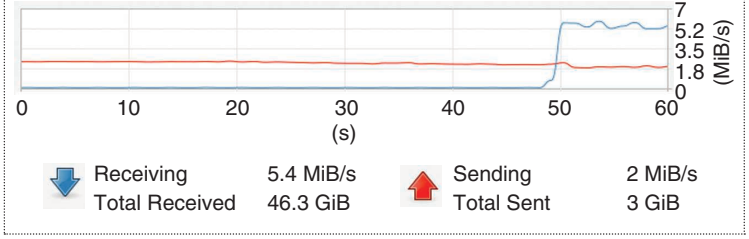

Figure 4. The network throughput before and after DDoS flooding attacks. MiB: mebibyte; GiB: gibibyte.

the buffer. A full buffer may cause a delay and even a drop in legitimate traffic. The communication channel between the control plane and the data plane can also be a target for man-in-the-middle attacks. This type of attack can modify or change the flow packets between the data and control planes, which enables an attacker to gain unauthorized access to the network devices. Even with the potential risks, SDNs facilitate rapid responses to the changing network conditions that we observed in 2020. ■

References

1. J. Novet. "Why Zoom has become the darling of remote workers during the COVID-19 crisis." CNBC. https://www.cnbc.com/2020/03/21/why-zoom-has-become-darling-of-remote-workers-amid-covid-19-outbreak.html (accessed July 8, 2020).
2. C. Labovitz. "Network traffic insights in the time of COVID-19: March 23-29 update." Nokia. https://www.nokia.com/blog/network-traffic-insights-time-covid-19-march-23-29-update/ (accessed July 8, 2020).
3. A. Walton. "Atlantic broadband network delivers high performance with heightened usage during COVID-19 crisis." Businesswire. https://www.businesswire.com/news/home/20200407005168/en/Atlantic-Broadband-Network-Delivers-High-Performance-With-Heightened-Usage-During-COVID-19-Crisis (accessed Oct. 2, 2020).
4. A. Morris. "U.K.'s EE sees 45% rise in chat app traffic amid COVID-19 lockdown." Lightreading. https://www.lightreading.com/services/uks-ee-sees-45–rise-in-chat-app-traffic-amid-covid-19-lockdown/d/d-id/759928 (accessed July 8, 2020).
5. H. Schulze. "2020 remote workforce security report." Bitglass. https://www.bitglass.com/?&utm_source=content (accessed July 20, 2020).
6. S. Jain et al., "B4: Experience with a globally-deployed software defined wan," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 3–14, 2013.doi:10.1145/2534169.2486019.
7. M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Machine-learning techniques for detecting attacks in SDN," in *Proc. 2019 IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT)*, pp. 277–281. doi: 10.1109/ICCSNT47585.2019.8962519.
8. M. Said Elsayed, N.-A. Le-Khac, S. Dev, and A. Delia Jurcut, "DDoSNet: A deep-learning model for detecting network attacks," in *Proc. 2020 IEEE 21st Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, pp. 391–396. doi: 10.1109/WoWMoM49955.2020.00072.
9. D. Marconett and S. Yoo, "FlowBroker: Market-driven multi-domain SDN with heterogeneous brokers," in *Proc. 2015 Opt. Fiber Commun. Conf. Exhibition (OFC)*, pp. 1–3. doi: 10.1364/OFC.2015.Th2A.36.
10. M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A novel SDN intrusion dataset," *IEEE Access*, vol. 8, pp. 165,263–165,284, Sept. 2020. doi: 10.1109/ACCESS.2020.3022633.

Mahmoud Said Elsayed is pursuing a Ph.D. in the School of Computer Science, University College Dublin, Dublin, Dublin 4, Ireland. His research interests include computer networks, network security, deep learning, and cloud computing. Elsayed received an M.E. in information security from Nile University, Giza, Egypt, in 2018. Contact him at mahmoud.abdallah@ucdconnect.ie.

Nhien-An Le-Khac is a lecturer in the School of Computer Science, University College Dublin, Dublin, Dublin 4, Ireland, where he also directs the M.Sc. program in forensic computing and cybercrime investigation and an international program for law enforcement officers specializing in cybercrime investigations. His research interests include cybersecurity and digital forensics; machine learning for security, fraud, and criminal detection; cloud security and privacy; and high-performance computing. Le-Khac received a Ph.D. in computer science from Institut National Polytechnique de Grenoble, France, in 2006. He has published more than 150 scientific papers in peer-reviewed journals and conferences, and he is an active chair and reviewer for many conferences and journals in related disciplines. He is a Member of IEEE. Contact him at an.lekhac@ucd.ie.

Anca Delia Jurcut is an assistant professor in the School of Computer Science, University College Dublin, Dublin, Dublin 4, Ireland. Her research interests include network and data security, security for the Internet of Things, security protocols, formal verification techniques, and applications of blockchain technologies in cybersecurity. Jurcut received a Ph.D. from the University of Limerick, Ireland, in 2013. Contact her at anca.jurcut@ucd.ie.